CLAIMS

What is claimed is:

1. A network configuration management system comprising:

a policy engine which generates configlets for a selected device; and

a combiner which combines the configlets to form at least one configuration file.

2. The system of Claim 1, wherein at least one of the configlets is vendor-neutral, further comprising:

a translator which translates the at least one vendor-neutral configlet to a vendor-specific configlet.

3. The system of Claim 1, wherein at least one of the configlets is vendor-specific.

4. The system of Claim 1, wherein the configlets are generated based on a selected feature set target level.

5. The system of Claim 4, wherein the policy engine generates the configlets using policies associated with the selected target level.

6. The system of Claim 5, further comprising:

a target hierarchy, wherein the policy engine generates the configlets using policies associated with the selected target level and its sub-target levels, as defined by the target hierarchy.

7. The system of Claim 5, wherein a policy comprises:

a condition; and

an action which the policy engine performs if the condition is true.

8. The system of Claim 7, wherein the policy action performed by the policy engine causes the policy engine to write to at least a partial configlet.

9. The system of Claim 5, wherein a policy further comprises:
a verification clause.

10. The system of Claim 9, wherein the verification clause is used to verify a configuration.

11. The system of Claim 10, further comprising:
a reverse-translator which produces configlets from a configuration file, wherein the verification clause verifies the configuration file by examining configlets produced by the reverse-translator.

12. The system of Claim 11, wherein the configuration is from a running network device.

13. The system of Claim 7, wherein a policy further comprises:
documentation.

14. The system of Claim 13, wherein the policy documentation comprises:
a reason; and
a description.

15. The system of Claim 5, wherein a second policy is dependent on a first policy, requiring that the second policy be evaluated after the first policy.

16. The system of Claim 15, wherein the first policy generates and stores a value to be used by the second policy.

17. The system of Claim 5, wherein a policy is written in a programming language.

18. The system of Claim 17, wherein the programming language is Perl with extensions.

19. The system of Claim 1, further comprising:

a configlet hierarchy, wherein a child configlet inherits properties which it does not define from its parent.

20. The system of Claim 1, further comprising:

a mapping function for mapping infrastructure data in a first format to a second format, the second format being recognizable by the policy engine.

21. The system of Claim 1, further comprising:

a loader for loading a configuration file to its intended device.

22. The system of Claim 21, further comprising:

a scheduler for scheduling the loading of a configuration to its intended device.

23. The system of claim 21, wherein multiple configurations are batched together to be scheduled for loading to their intended devices.

24. The system of Claim 1, wherein a device is one of the group comprising: a router, a switch, a bridge, a firewall, a hub, an interface, a web hosting server, a DNS server and a virtual interface.

25. The system of Claim 1, further comprising:

a configuration archive.

26. The system of Claim 25, wherein generated configurations are stored in the archive.

27. The system of Claim 25, wherein configurations are uploaded from devices and are stored in the archive.

28. The system of Claim 1, further comprising:

a reverse-translator which produces vendor-neutral configlets from a configuration file, wherein a configuration is read back from a device.

29. The system of Claim 28, wherein a first device using a first configuration format is replaced with a second device using a second configuration format, and wherein the first device's configuration is read in and reverse-translated into vendor-neutral configlets, the vendor-neutral configlets then being translated into a configuration formatted for the second device.

30. The system of Claim 1, wherein the system retains login information to the devices, such that a user desiring to connect to a device must log in to the system, the system connecting to the device.

31. The system of Claim 30, wherein the system passes commands from the user to the device, and responses from the device to the user.

32. The system of Claim 1, wherein the policy engine generates configlets for plural selected devices.

33. The system of Claim 1, wherein at least one of said configuration files comprises a full configuration.

34. The system of Claim 1, wherein at least one of said configuration files comprises a partial configuration.

35. A method for managing network configurations, comprising:

generating configlets for a selected device; and

combining the configlets to form at least one configuration file.

36. The method of Claim 35, wherein at least one of the configlets is vendor-neutral, further comprising:

translated the at least one vendor-neutral configlet to a vendor-specific configlet.

37. The method of Claim 35, wherein at least one of the configlets is vendor-specific.

38. The method of Claim 35, wherein configlets are generated based on a selected feature set target level.

39. The method of Claim 38, wherein generating the configlets comprises evaluating policies associated with the selected target level.

40. The method of Claim 39, further comprising:

defining a target hierarchy, generating the configlets comprises evaluating policies associated with the selected target level and its sub-target levels, as defined by the target hierarchy.

41. The method of Claim 39, wherein evaluating a policy comprises:

evaluating a condition described by the policy; and

performing an action described by the policy if the condition is true.

42. The method of Claim 41, wherein performing the action comprises writing to at least a partial configlet.

43. The method of Claim 39, further comprising:

verifying a configuration.

44. The method of Claim 43, wherein the configuration is a configuration from a running network device.

45. The method of Claim 44, further comprising:

reverse-translating a configuration file into configlets, wherein verifying the configuration file comprises examining the reverse-translated configlets.

46. The method of Claim 39, further comprising:

defining policy dependencies such that a second policy dependent on a first policy must be evaluated after the first policy.

47. The method of Claim 46, wherein the first policy generates and stores a value to be used by the second policy.

48. The method of Claim 39, wherein a policy is written in a programming language.

49. The method of Claim 48, wherein the programming language is Perl with extensions.

50. The method of Claim 35, further comprising:

defining a configlet hierarchy, wherein a child configlet defines properties which it does not inherit from its parent.

51. The method of Claim 35, further comprising:

mapping infrastructure data in a first format to a second format, the second format being recognizable by the policy engine.

52. The method of Claim 35, further comprising:

loading a configuration file to its intended device.

53. The method of Claim 52, further comprising:

scheduling the loading of a configuration to its intended device.

54. The method of claim 52, batching together multiple configurations to be scheduled for loading to their intended devices.

55. The method of Claim 35, wherein a device is one of the group comprising: a router, a switch, a bridge, a firewall, a hub, an interface and a virtual interface.

56. The method of Claim 35, further comprising:

archiving configurations in a configuration archive.

57. The method of Claim 56, further comprising:

storing generated configurations in the archive.

58. The method of Claim 56, further comprising:

uploading a configuration from a device; and

storing the uploaded configuration in the archive.

59. The method of Claim 35, further comprising:

a reverse-translator which produces vendor-neutral configlets from a configuration file, wherein a configuration is read back from a device.

60. The method of Claim 59, comprising:

upon replacing a first device using a first configuration format with a second device using a second configuration format,

uploading the first device's configuration;

reverse-translating the uploaded configuration into vendor-neutral configlets; and

translating the vendor-neutral configlets into a configuration formatted for the second device.

61. The method of Claim 35, further comprising:

retaining device login information;

maintaining user accounts;

allowing a user to login to the user's account;

logging into a device; and

passing information between the user and the device as if the user were logged onto the device.

62. The method of Claim 61, wherein the maintained device logins and passwords are encrypted.

63. The method of Claim 35, wherein the policy engine generates configlets for plural selected devices.

64. The method of Claim 35, wherein at least one of said configuration files comprises a full configuration.

65. The method of Claim 35, wherein at least one of said configuration files comprises a partial configuration.

66. A method of accessing a configuration setup on a network device, comprising:

maintaining login information for access to the device in the device and in a configuration server;

maintaining, in the server, login information for access from a user to the server and device access rights for the user; and

accessing the configuration setup of the device by a user through the server by the user accessing the server and the server accessing the device.

67. The method of Claim 66, wherein the maintained device login information is encrypted.

68. The method of Claim 66, further comprising:

monitoring communications between the user and the device.

69. The method of Claim 66, further comprising:

recording communications between the user and the device.

70. A configuration server for enabling configuration set up of network devices, comprising:

storage including

login information for access to the device,

login information for access from a user to the server, and

device access rights for the user; and

an access processor enabling a user to set up configuration of the device through the server by the user accessing the server and the server accessing the device.

71. The server of Claim 70, wherein the maintained device login information is encrypted.

72. The server of Claim 70, further comprising:

a monitor which monitors communications between the user and the device.

73. The server of Claim 70, further comprising:

a recorder for recording communications between the user and the device.

74. A system for managing network configurations, comprising:

means for generating configlets based on a selected feature set target level and a selected device; and

means for translating and combining the configlets to form vendor-dependent configuration files.

75. A system of accessing a configuration setup on a network device, comprising:

means for maintaining login information for access to the device in the device and in a configuration server;

means for maintaining, in the server, login information for access from a user to the server and device access rights for the user; and

means for accessing the configuration setup of the device by a user through the server by the user accessing the server and the server accessing the device.